IN THE SPECIFICATION:

The specification as amended below with replacement paragraphs shows added text with underlining and deleted text with ~~strikethrough~~.

Please REPLACE the paragraph beginning at page 10, line 8, with the following paragraph:

Described briefly below is the security of the random mask value method. In the random mask value method, the Sbox, wi', of FIGURES 13A and 13B in each round shown in FIGURE 10 and in FIGURE 19 as described later changes in accordance with a random number. Thus, the content of the SBox can not be known by the DPA. That is, since the condition of the case 1 above that the SBox is known is not satisfied, the dissipated power curves measured at the predetermined timing at the measured point A shown in FIGURE 8 can not be divided into G0 and G1 in accordance with the equations (1) and (2). Thus, the encryption device employing the random mask value method is secure against the DPA. Similarly, with respect to the conditions of the cases 2 and 3 above, the random element which changes each time in the measuring is combined at the measured point B at the output of the key XOR function and at the measured point C at the input to an Sbox. Thus, the condition that the key K is fixed is not satisfied. Thus, it is secure against the DPA.

Please REPLACE the paragraph beginning at page 12, line 23, with the following paragraph:

[1110] XOR the operation output from Step [1109] ~~using~~ with the output Rout from the mask value generation, and a resultant ciphertext is provided as an ultimate output.

Please REPLACE the paragraph beginning at page 30, line 7, with the following paragraph:

Thus, the amount of the available ROM required for the SBoxes used in the encryption device 400 of FIGURE 29 can be reduced to one sixteenth of that in the encryption device 300 of FIGURE 27. Therefore, the ROM area required for the SBoxes in the encryption device 400 of FIGURE 29 which satisfies the equations (13) can be reduced to only 1/(16N) of that in the encryption device 300 of FIGURE 27.

Please REPLACE the paragraph beginning at page 36, line 2, with the following paragraph:

Next, in the adjacent bit model expressed by the equation (6) which is applicable for the DPA, it is assumed that the number of different SBox sets to used in the Subbyte is limited to one in accordance with q = 2 and the equations (13), for the purpose of the explanation. It is known that the adjacent bit model is appropriate for approximating a voltage in a low cost smart card. If this model is applicable, the key information which can not be analyzed for decryption in the arbitrary model above can be analyzed for decryption. In the Subbyte in the 0-th round in the encryption devices 400 and 500 of FIGURES 29 and 31, respectively, the DPA is applied at the timing (at the predetermined timing at the measured point C shown in FIGURE 9) of loading the input value of each SBox, ~~to~~ and thereby the key Ki can be determined for decryption in the amount of computation proportional to $2^{128-(15/16)H}$, where $H = h_0 + h_1 + ... + H_{15}$. The value h_j is defined as described below. It is assumed that the input mask values of the j-th SBox are $c_{0,j}$ and $c_{1,j}$,

for $WC_j = C_{0,j} \oplus C_{1,j} = (W_{cj},7\ WC_{j,6} ... WC_{j,0})_2$,

hj = (number of e's such that $WC_{j,e}=0$ for e=0,1,...7).

+(number of e's such that $WC_{j,e} = WC_{j,e+1}= 1$ for e=0,1,...7),

where $WC_{j,e}$ = 0 or 1. The value j represents the ordinal number of an SBox. The value e represents a bit position.